

Claims

1    1. In a data processing operation having stored data in  
2    a plurality of data files, a system for protecting said  
3    data files from unauthorized users comprising:

4        means for receiving user requests for access to data  
5    files;

6        means for determining whether said requests are  
7    unauthorized intrusions into said requested data files;  
8    and

9        means responsive to a determination that a request  
10   is unauthorized for destroying the requested data files.

1    2. The data processing operation system of claim 1  
2    further including means for storing for each of said  
3    plurality of data files, a backup file inaccessible to  
4    user requests.

1    3. The data processing operation system of claim 2  
2    further including means for reloading a backup file for  
3    each destroyed file.

1    4. The data processing operation system of claim 1  
2    wherein said means for determining whether said user  
3    requests are unauthorized intrusions include:

4        means for determining whether a user access  
5    identification code has been denied; and

6        means for determining whether the user has copied  
7    the requested files.

1       5. In a communication network with access to a plurality  
2       of network sites each having stored data in a plurality  
3       of data files accessible in response to requests from  
4       users at other sites in the network, a system for  
5       protecting said network site data files from unauthorized  
6       users comprising:

7              means associated with a network site for  
8       receiving user requests for access to data files;

9              means at said network site for determining whether  
10      said user requests are unauthorized intrusions into said  
11      requested data files; and

12             means at said network site responsive to a  
13      determination that a request is unauthorized for  
14      destroying the requested data files.

1       6. The communication network system of claim 5 further  
2       including means for storing for each of said plurality of  
3       data files at said network site, a backup file  
4       inaccessible to user requests.

1       7. In a World Wide Web communication network with access  
2 to a plurality of open Web sites each having stored data  
3 in a plurality of data files accessible in response to  
4 requests from users at stations throughout the Web, a  
5 system for protecting said open Web site data files from  
6 unauthorized users comprising:

7              means associated with an open Web site for  
8 receiving user requests for access to data files;

9              means at said open Web site for determining whether  
10 said user requests are unauthorized intrusions into said  
11 requested data files; and

12             means at said open Web site responsive to a  
13 determination that a request is unauthorized for  
14 destroying the requested data files.

1       8. The World Wide Web communication network system of  
2 claim 7 further including means for storing for each of  
3 said plurality of data files at said open Web site, a  
4 backup file inaccessible to user requests.

1       9. The World Wide Web communication network system of  
2 claim 8 further including means for reloading a backup  
3 file for each destroyed file.

1   10. In a data processing operation having stored data in  
2   a plurality of data files, a method for protecting said  
3   data files from unauthorized users comprising:  
4         receiving user requests for access to data files;  
5         determining whether said requests are unauthorized  
6         intrusions into said requested data files; and  
7         destroying the requested data files responsive to a  
8   determination that a request is unauthorized.

1   11. The data processing method of claim 10 further  
2   including the step of storing for each of said plurality  
3   of data files, a backup file inaccessible to user  
4   requests.

1   12. The data processing method of claim 11 further  
2   including the step of reloading a backup file for each  
3   destroyed file.

1   13. The data processing method of claim 10 wherein said  
2   step of determining whether said user requests are  
3   unauthorized intrusions includes:  
4         determining whether a user access identification  
5   code has been denied; and  
6         determining whether the user has copied the  
7   requested files.

1   14. In a communication network with access to a  
2   plurality of network sites each having stored data in a  
3   plurality of data files accessible in response to  
4   requests from users at other sites in the network, a  
5   method for protecting said network site data files from  
6   unauthorized users comprising:

7           receiving user requests for access to data files at  
8   a network site;

9           determining at said network site whether said user  
10   requests are unauthorized intrusions into said requested  
11   data files; and

12          destroying the requested data files responsive to a  
13   determination that a request is unauthorized.

1   15. The communication network method of claim 14 further  
2   including the step of storing for each of said plurality  
3   of data files at said network site, a backup file  
4   inaccessible to user requests.

1   16. The communication network method of claim 15 further  
2   including the step of reloading a backup file for each  
3   destroyed file.

1   17. In a World Wide Web communication network with  
2 access to a plurality of open Web sites each having  
3 stored data in a plurality of data files accessible in  
4 response to requests from users at stations throughout  
5 the Web, a method for protecting said open Web site data  
6 files from unauthorized users comprising:

7         receiving user requests for access to data files at  
8 said open Web site;

9         determining whether said user requests are  
10 unauthorized intrusions into said requested data files at  
11 said open Web site; and

12         destroying the requested data files at said open Web  
13 site responsive to a determination that a request is  
14 unauthorized.

1   18. The World Wide Web communication network method of  
2 claim 17 further including the step of storing for each  
3 of said plurality of data files at said open Web site, a  
4 backup file inaccessible to user requests.

1   19. The World Wide Web communication network method of  
2 claim 18 further including the step of reloading a backup  
3 file for each destroyed file.

1   20. The World Wide Web communication network method of  
2 claim 17 wherein said step of determining whether said  
3 user requests are unauthorized intrusions includes:

4         determining whether a user access identification  
5 code has been denied; and

6         determining whether the user has copied the  
7 requested files.

1       21. A computer program having code recorded on a  
2 computer readable medium for protecting data files from  
3 unauthorized users in a data processing operation having  
4 stored data in a plurality of data files, said program  
5 comprising:

6           means for receiving user requests for access to data  
7 files;

8           means for determining whether said requests are  
9 unauthorized intrusions into said requested data files;  
10 and

11          means responsive to a determination that a request  
12 is unauthorized for destroying the requested data files.

1       22. The computer program of claim 21 further including  
2 means for storing for each of said plurality of data  
3 files, a backup file inaccessible to user requests.

1       23. The computer program of claim 22 further including  
2 means for reloading a backup file for each destroyed  
3 file.

1       24. The computer program of claim 21 wherein said means  
2 for determining whether said user requests are  
3 unauthorized intrusions include:

4           means for determining whether a user access  
5 identification code has been denied; and

6           means for determining whether the user has copied  
7 the requested files.

1   25. A computer program having code recorded on a  
2 computer readable medium for protecting data files from  
3 unauthorized users in a communication network with access  
4 to a plurality of network sites each having stored data  
5 in a plurality of data files accessible in response to  
6 requests from users at other sites in the network, said  
7 program comprising:

8                 means associated with a network site for  
9 receiving user requests for access to data files;

10                means at said network site for determining whether  
11 said user requests are unauthorized intrusions into said  
12 requested data files; and

13                means at said network site responsive to a  
14 determination that a request is unauthorized for  
15 destroying the requested data files.

1   26. The computer program of claim 25 further including  
2 means for storing for each of said plurality of data  
3 files at said network site, a backup file inaccessible to  
4 user requests.

1   27. A computer program having code recorded on a  
2   computer readable medium for protecting open Web sites in  
3   a World Wide Web communication network with access to a  
4   plurality of open Web sites each having stored data in a  
5   plurality of data files accessible in response to  
6   requests from users at stations throughout the Web, said  
7   program comprising:

8         means associated with an open Web site for  
9         receiving user requests for access to data files;

10        means at said open Web site for determining whether  
11        said user requests are unauthorized intrusions into said  
12        requested data files; and

13        means at said open Web site responsive to a  
14        determination that a request is unauthorized for  
15        destroying the requested data files.

1   28. The computer program of claim 27 further including  
2   means for storing for each of said plurality of data  
3   files at said open Web site, a backup file inaccessible  
4   to user requests.

1   29. The computer program of claim 28 further including  
2   means for reloading a backup file for each destroyed  
3   file.

1   30. The computer program of claim 27 wherein said means  
2   for determining whether said user requests are  
3   unauthorized include:

4         means for determining whether a user access  
5         identification code has been denied; and

6         means for determining whether the user has copied  
7         the requested files.